

Datenbanken und Datensicherheit

Prof. Dr. rer. nat. Peter Gerwinski

27. November 2024

Datenbanken und Datensicherheit

<https://gitlab.cvh-server.de/pgerwinski/dbs>

1 Einführung

2 Kurzeinführung Unix

3 Kurzeinführung TCP/IP

3.1 MAC-Adressen

3.2 IP-Adressen

3.3 TCP- und UDP-Ports

3.4 Protokolle

3.5 Routing

3.6 Netzwerkanalyse

3.7 SSH

3.8 X11 und VNC

3.9 GNU screen

3.10 Firewall

4 Relationale Datenbanken

...



Änderungen
vorbehalten

3.7 SSH

- Sicheres¹ Arbeiten auf einem entfernten Rechner
- `ssh <Rechner>`
- `-C`: Komprimierung
- `-L`: lokalen Port auf Remote-Port umleiten
- `-R`: Remote-Port auf lokalen Port umleiten

- Beim ersten Verbinden:
öffentlichem Schlüssel des entfernten Rechners prüfen
(mit `ssh-keygen` abrufen, wird in `.ssh/known_hosts` hinterlegt)
- Anstelle eines Passwortes: eigenes Schlüsselpaar erzeugen,
öffentlichem Schlüssel in `.ssh/authorized_keys` hinterlegen
- Zusätzliche Sicherheit:
eigenen geheimen Schlüssel durch Passwort schützen
- Passwort nicht jedes Mal neu eingeben:
SSH-Agent (`ssh-add`)

¹gemäß Stand der Technik, so sicher wie z. Zt. überhaupt möglich

3.8 X11 und VNC

- Grafik-Bildschirm und Eingabegeräte über's Netz
- `DISPLAY`-Variable: X-Server: Rechner und Bildschirm
- `ssh -X`, `ssh -Y`: X11-Forwarding

Warnung: Der entfernte Rechner bekommt Zugriff auf den X-Server und kann insbesondere Tastatureingaben mitlesen!

Für Details siehe: X11-SECURITY-Erweiterungen:

<https://www.x.org/wiki/Development/Documentation/Security/>

- VNC = Virtual Network Computing
- VNC-Server stellt Bildschirminhalt zur Verfügung
 - entweder: eigener, virtueller X11-Server
 - oder: ruft Inhalt von anderem (X11-) Bildschirm ab
- VNC-Client ruft Bildschirminhalt ab und stellt ihn dar
 - z. B. per X11
 - z. B. per Web-Interface: noVNC

3.9 GNU screen

- Text-Bildschirm und Eingabegeräte über's Netz
- `Ctrl+A c`: neues Fenster (create)
- `Ctrl+A Leertaste`: nächstes Fenster
- `Ctrl+A 3`: Fenster Nr. 3
- `Ctrl+A ESC`: hochscrollen, suchen, markieren (copy)
- `Ctrl+A]`: einfügen (paste)
- `Ctrl+A d`: von `screen` ablösen (detach)
- `screen -x`: an laufenden `screen` andocken, auch geteilt
- Ablösen/Andocken, auch geteilt, für Grafik: `VNC`, `x2go`
- Alternative: `tmux`

3.10 Firewall

- ~~• magische Hardware und/oder Software, die uns vor allen Angriffen schützt~~
- Paketfilter (Internet- und Transportschicht: IP-Adressen, Port-Nummern)

3.10 Firewall

- ~~magische Hardware und/oder Software,
die uns vor allen Angriffen schützt~~
 - Paketfilter (Internet- und Transportschicht: IP-Adressen, Port-Nummern)
 - Stateful Packet Inspection (Transportschicht)
 - Deep Packet Inspection (Anwendungsschicht)
 - Proxy (Anwendungsschicht)
 - Anfragen verstehen,
stellvertretend für die Anwendung beim Server anfragen
- > mehrere Anfragen bündeln: weniger Netzlast
- > Inhalte filtern: Malware erkennen,
aber auch „politisch unerwünschte“ Inhalte

Anwendung: HTTP, SMTP, ...
Transport: TCP-/UDP-Ports, ICMP
Internet: IP-Adresse
Netzwerkzugang: Hardware-/MAC-Adresse

4 Relationale Datenbanken

4.1 Einführung in DBMS

Datenbank-Management-System (DBMS): z. B. PostgreSQL, MariaDB

- Datenbanken „von außen“ verwalten (z. B. auflisten)
- Schnittstelle für Zugriff auf Datenbank
- **in hohem Maße herstellerspezifisch**

```
root@cassini:~# su - postgres
postgres@cassini:~$ psql
psql (15.3 (Debian 15.3-0+deb12u1))
Geben Sie »help« für Hilfe ein.
```

```
postgres=# help
Dies ist psql, die Kommandozeilenschnittstelle für PostgreSQL.
Geben Sie ein:  \copyright für Urheberrechtsinformationen
                 \h für Hilfe über SQL-Anweisungen
                 \? für Hilfe über interne Anweisungen
                 \g oder Semikolon, um eine Anfrage auszuführen
                 \q um zu beenden

postgres=#
```


4 Relationale Datenbanken

4.1 Einführung in DBMS

Datenbank-Management-System (DBMS): z. B. PostgreSQL, MariaDB

- Datenbanken „von außen“ verwalten (z. B. auflisten)
- Schnittstelle für Zugriff auf Datenbank
- **in hohem Maße herstellerspezifisch**

```
postgres=# \?  
Allgemein  
  \copyright           PostgreSQL-Urheberrechtinformationen zeigen  
  \crosstabview [SPALTEN] Anfrage ausführen und Ergebnis als Kreuztabelle  
                        anzeigen  
  \errverbose          letzte Fehlermeldung mit vollen Details anzeigen  
  \g [(OPT)] [DATEI]   SQL-Anweisung ausführen (und Ergebnis in Datei  
                        oder |Pipe schreiben); ...  
  ...                  ...  
  \q                   psql beenden  
  ...                  ...
```

```
postgres=#
```

4 Relationale Datenbanken

4.1 Einführung in DBMS

Datenbank-Management-System (DBMS): z. B. PostgreSQL, MariaDB

- Datenbanken „von außen“ verwalten (z. B. auflisten)
- Schnittstelle für Zugriff auf Datenbank
- **in hohem Maße herstellerspezifisch**

```
postgres=# \l
```

Liste der Datenbanken					
Name	Eigentümer	Kodierung	Sortierfolge	Zeichentyp	...
postgres	postgres	UTF8	de_DE.UTF-8	de_DE.UTF-8	
template0	postgres	UTF8	de_DE.UTF-8	de_DE.UTF-8	
template1	postgres	UTF8	de_DE.UTF-8	de_DE.UTF-8	
(3 Zeilen)					...

```
postgres=#
```

4 Relationale Datenbanken

4.2 Einführung in SQL

Datenbank-Abfragesprache: Structured Query Language (SQL)

- Datenbanken „von innen“ verwalten, z. B. anlegen und wieder löschen
- Daten in der Datenbank bearbeiten
- **in hohem Maße standardisiert**

```
postgres=# create database testdb;  
CREATE DATABASE  
postgres=# create user dbsadmin with password '####';  
CREATE ROLE  
postgres=# create user dbs with password '####';  
CREATE ROLE  
postgres=# ALTER DATABASE testdb OWNER TO dbsadmin;  
ALTER DATABASE  
postgres=# \q  
postgres@cassini:~$
```

4 Relationale Datenbanken

4.2 Einführung in SQL

Datenbank-Abfragesprache: Structured Query Language (SQL)

- Datenbanken „von innen“ verwalten, z. B. anlegen und wieder löschen
- Daten in der Datenbank bearbeiten
- **in hohem Maße standardisiert**

```
$ psql -h localhost -U dbadmin -W testdb
```

```
Password: ####
```

```
psql (15.5 (Debian 15.5-0+deb12u1))
```

```
SSL-Verbindung (Protokoll: TLSv1.3, Verschlüsselungsmethode: TLS_AES_256_G
```

```
Geben Sie »help« für Hilfe ein.
```

```
testdb=> grant select, insert, update on tier to dbs;
```

```
GRANT
```

```
testdb=> \q
```

4 Relationale Datenbanken

4.2 Einführung in SQL

Datenbank-Abfragesprache: Structured Query Language (SQL)

- Datenbanken „von innen“ verwalten, z. B. anlegen und wieder löschen
- Daten in der Datenbank bearbeiten
- **in hohem Maße standardisiert**

```
$ psql -h localhost -U dbs -W testdb
```

```
Passwort: ####
```

```
psql (15.5 (Debian 15.5-0+deb12u1))
```

```
SSL-Verbindung (Protokoll: TLSv1.3, Verschlüsselungsmethode: TLS_AES_256_G
```

```
Geben Sie »help« für Hilfe ein.
```

```
testdb=> drop table tier;
```

```
FEHLER: Berechtigung nur für Eigentümer der Tabelle tier
```

```
testdb=>
```

4 Relationale Datenbanken

4.2 Einführung in SQL

Datenbank-Abfragesprache: Structured Query Language (SQL)

Literatur: z. B. https://de.wikibooks.org/wiki/Einführung_in_SQL

Wichtige SQL-Befehle:

- **CREATE** – Datenbanken, Tabellen usw. anlegen
- **DROP** – Datenbanken, Tabellen usw. löschen
- **SELECT** – Daten abfragen
- **INSERT INTO ... VALUES** – Daten eingeben
- **UPDATE** – Daten ändern
- **DELETE FROM** – Daten löschen